Department of Homeland Security Daily Open Source Infrastructure Report for 8 May 2008

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
http://www.dhs.gov/

- The Saint Louis Dispatch reports that according to Food and Drug Administration records, 400 shipments of Chinese seafood to the U.S. were sent back due to contamination or other issues despite the fact that less than 1 percent of all imports were inspected. (See item **15**)
- TG Daily reports that several hundred to possibly a thousand laptops are missing from the U.S. State Department, according to an internal audit. Many likely contain classified information, and as many as 400 computers belonged to the Anti-Terrorism Assistance Program which provides counterterrorism training to other nations. (See item **29**)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *May 6, Reuters* – (National) **Sierra Club threatens suits over coal power plants.** The Sierra Club sent letters on Tuesday threatening to file suit to stop construction of eight coal-fired power plants in six states because, the environmental group claims, they violate the Clean Air Act. In February, a federal appeals court in Washington ruled that the U.S. Environmental Protection Agency violated the Clean Air Act in not setting mandatory cuts for mercury emissions of power plants. The suits would be filed in the federal districts where the proposed power plants would be located, said the director of the Sierra Clubs effort to stop coal power plants. The suits would seek to require the plants to go back to state permitting agencies for new permits that meet the tougher emission standards. The Sierra Club said until capturing and sequestering carbon dioxide emissions is proven feasible and affordable, no more coal plants should be built.

About 30 coal-fired plants may be affected by the Sierra Club suits, the director said.
Source: http://www.reuters.com/article/environmentNews/idUSN0651739020080507?pageNumber=1&virtualBrandChannel=0

2. *May 6, U.S. Department of Energy* – (National) **DOE awards $126.6 million for two more large-scale carbon sequestration projects.** The U.S. Department of Energy (DOE) Tuesday announced awards of more than $126.6 million to the West Coast Regional Carbon Sequestration Partnership and the Midwest Regional Carbon Sequestration Partnership for the Departments fifth and sixth large-scale carbon sequestration projects. These industry partnerships, which are part of DOEs Regional Carbon Sequestration Partnership, will conduct large volume tests in California and Ohio to demonstrate the ability of a geologic formation to safely, permanently, and economically store more than one million tons of carbon dioxide.
Source: http://www.energy.gov/news/6231.htm

[Return to top]

Chemical Industry Sector

Nothing to Report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *May 7, Rutland Herald* – (Vermont) **NRC hits Yankee with noncited violation over cooling tower.** The U.S. Nuclear Regulatory Commission (NRC) has issued Entergy Nuclear a "noncited violation" for failing to follow industry recommendations last year regarding potential problems at cooling towers. A noncited violation means there will be no permanent penalty against Entergy for the August 21 partial collapse of one of its cooling towers. A noncited violation also means it would not be considered in any future review of the plant, should problems develop. An NRC spokesman said federal inspectors found the cooling tower collapse had no significant safety implication for the operation of the plant. "We want to make sure it doesn't happen again," he said, noting that federal regulators had asked for the company to do a root-cause analysis of what was behind the collapse, and for the company to develop changes to address the problems. "They have done just that," he said.
Source: http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20080507/NEWS04/805070388/1003/NEWS02

4. *May 6, Carlsbad Current-Argus* – (Idaho) **Its official: Areva selects Idaho.** A French company's decision to build a $2 billion uranium enrichment facility in Idaho was made official Tuesday. Areva NC Inc. will build its first U.S. uranium enrichment facility in Bonneville County, Idaho, according to a press release issued Tuesday morning. According to the press release, the decision was made after an extensive analysis of

several potential sites throughout the U.S. Areva will now seek approval from federal, state, and local agencies, including a license from the U.S. Nuclear Regulatory Commission, to construct and operate the facility.
Source: http://www.currentargus.com/ci_9175422

5. *May 6, Associated Press* – (International) **Russia, U.S. sign civil nuclear pact.** Russian and U.S. officials signed a key agreement on civilian nuclear power Tuesday that could give Washington access to Russian technology and potentially hand Moscow lucrative deals on storing spent fuel. But the agreement ran into immediate trouble on Capitol Hill, where two senators said they would try to block it. The two senators are circulating a letter that will urge the U.S. president not to send the pact to Congress. The deal will give the U.S. access to Russian state-of-the art nuclear technology. The U.S. is especially interested in developments in areas including fast-neutron reactors and recycling nuclear fuel. The deal could also help Russia in its efforts to establish an international nuclear fuel storage facility by importing and storing spent fuel.
Source: http://www.philly.com/philly/wires/ap/news/world/20080506_ap_russiaussigncivilnuclearpact.html

[Return to top]

Defense Industrial Base Sector

6. *May 6, Strategy Page* – (National) **Aegis ABM gets big boost.** Japan has agreed to help the U.S. develop a multiple warhead version of the SM-3 anti-ballistic missile system. This system, the RIM-161A, also known as the Standard Missile 3 (SM-3), has a range of over 310 miles and max altitude of about 100 miles. The Standard 3 is based on the failed anti-missile version of the Standard 2, and costs over nine million dollars each. The SM-3 Block IIA version would have three LEAP kill vehicles in the warhead. Each would be lighter than the current one, but would be just as effective. Other stages of the SM-3 Block IIA will be heavier, a plan already in the works. This version would have a longer range, about 620 miles, and higher operating altitude. The SM-3 Block IIA is not expected to be ready to go for another six years or so.
Source: http://www.strategypage.com/htmw/htada/articles/20080506.aspx

7. *May 2008, National Defense Magazine* – (National) **Ground robots place in military at risk, experts warn.** The Army's Future Combat Systems (FCS) and the Navy EOD next generation bomb platforms are the two programs driving ground robotics development in the military. FCS plans include mules, which will autonomously carry loads for soldiers, and small reconnaissance robots, designed to enter buildings and send back pictures to soldiers. FCS future, however, remains in doubt. The program faces yearly funding cuts and has yet to face a preliminary design review and a limited user test. For some EOD robots, maintaining communication links proved to be difficult. As a result, this application of the technology has not progressed much during the past seven years. Armed ground robots are another application that is making little progress. Most agree that it is too soon to introduce them into battlefields. Three remotely controlled armed robots were sent to Iraq last summer, but have not seen action. The

director of the joint ground robotics enterprise at the office of the undersecretary of defense said the military will "start moving in a more deliberate and ambitious direction" when it comes to ground robots. One way to move the ground programs forward will be to get them to work together in "collective" operations with other unmanned systems.
Source: http://www.nationaldefensemagazine.org/issues/2008/May/Ground.htm

8. *May 2008, National Defense Magazine* – (National) **Navy to field a family of next-generation bomb disposal robots.** The Navy will field a family of bomb disposal robots to replace the ad hoc commercial systems being used today. Plans call for a suite of small, medium, and large robots that will be able to perform a variety of missions depending on their size. The Navy wants a scalable common chassis – not unlike what the Army is building for its Future Combat System vehicles. Important improvements to future EOD robots will be the open architecture systems – so robots can use "plug-and-play" attachments – and a common controller. Robots will have modular designs, allowing broken items to be swapped out quickly. Meanwhile, work continues to improve the capabilities of the robots being used today. The new family of robots will not be fielded until 2013, so Talons, manufactured by Foster-Miller, and iRobots Packbots will be in use for another five years. One key improvement has been the controllers, which resemble those of Sony PlayStation. The new controller allows EOD technicians to plug into a USB port and sit back so the other members of the team in the vehicle can see the screen.
Source: http://www.nationaldefensemagazine.org/issues/2008/May/Navy.htm

[Return to top]

Banking and Finance Sector

9. *May 6, IT Business Edge* – (National) **Trove of stolen data discovered.** Web security company Finjan has alerted international banks and police after finding a huge stash of stolen business and personal data on what it is calling a "crimeserver," reports Reuters. In operation just three weeks, the server held 1.4 gigabytes of information from 5,388 unique log files. The data included company personnel files, insurance records, Social Security numbers, medical records, login and transaction information with not only credit card and account numbers but also passwords and security codes, according to Government Computer News. It says two similar, but smaller servers have been found since. The server was not secured, so it was accessible to anyone who could find it, though the Russian man who owned it apparently was moving it regularly between Russia, China, Hong Kong and finally Singapore, where it was shut down. Finjan has notified more than 40 major international financial institutions in the United States, Europe and India that customers' information was compromised, as well as the FBI and law enforcement agencies around the world.
Source: http://www.itbusinessedge.com/blogs/hdw/?p=2143

10. *May 6, KCAL 9 Los Angeles* – (California) **Suspicious package found at Sherman Oaks Center.** A bomb squad was called out Tuesday to investigate a suspicious package left outside a Washington Mutual bank branch in Sherman Oaks, California. A

note on the package read, “Do not get close,” according to reports. The bank was already closed, but a Trader Joes store and a produce market was evacuated and traffic was diverted away from the area. “Were still trying to figure out what it is,” the watch commander at the Van Nuys police station said of the package.
Source: http://cbs2.com/local/Suspicious.Package.Sherman.2.717640.html

[Return to top]

Transportation Sector

11. *May 7, USA Today* – (National) **Program to allow air travelers to speed through Customs checks.** Starting Monday, air travelers can sign up to speed through Customs checkpoints at select U.S. airports when they return from trips abroad. A government program called Global Entry will enable U.S. citizens and permanent residents to avoid the long lines that often greet them when they get off airplanes arriving from international destinations. People who pass a background check and pay $100 to enroll will enter a separate Customs line at certain airports. They will swipe their passport at a kiosk instead of having it read by a Customs officer and electronically answer questions similar to those on a Customs declaration form. If no problems arise, they will be cleared through Customs. The program will start operating June 10 at three airports — Washington Dulles, Houston Intercontinental and New York’s Kennedy. Customs and Border Protection expects it will expand to 17 other major U.S. airports, the program director says. Wagner of Customs and Border Protection says Global Entry is aimed at people who take at least four international trips a year.
Source: http://www.usatoday.com/travel/flights/2008-05-06-travelers_N.htm

12. *May 6, Associated Press* – (Minnesota) **State to close parts of Duluth bridge to strengthen gussets.** Minnesota transportation officials on Tuesday announced a partial closing of the Blatnik Bridge that connects Duluth and Superior, Wisconsin, after finding that gusset plates at eight spots on the bridge did not meet load requirements. Traffic on the bridge will be reduced from four lanes to two while the plates are reinforced, with work expected to be complete by the middle of June. The bridge, also known as the High Bridge, opened in 1961. Reconstruction from 1992 to 1994 added a new, thicker deck and heavier railings, and an analysis found that the gussets were not sufficient for the added weight, Minnesota Department of Transportation (MnDOT) said. The bridge, which carries I-535 over the St. Louis River, carries about 29,500 vehicles a day, MnDOT said. A fact sheet said the bridge is the states second-longest at 7,980 feet. Minnesota’s bridges have been under close scrutiny since the Minneapolis bridge collapse in August, a catastrophe blamed in part on too-thin gusset plates. The partial Blatnik closure comes just a few weeks after the DeSoto Bridge in St. Cloud was shut down because of warped gusset plates.
Source: http://www.chicagotribune.com/news/chi-ap-mn-duluthbridge-repa,0,5490311.story

[Return to top]

Postal and Shipping Sector

13. *May 6, WIVB 4 Buffalo* – (New York) **Buffalo Police continue to investigate suspicious package incident.** In Buffalo, New York, police continue to investigate an incident Monday night that shut down an entire city block. At around 4:30 Monday afternoon, the Erie County Bomb Squad found five envelope size packages inside a UPS storage box. Upon further investigation, the Bomb Squad commander and his crew eased fears and concerns the parcels contained explosives. One day later, police and bomb squad investigators are not giving any information about the packages contents or whether they are looking for the man whom someone reported as acting "suspicious." Source: http://www.wivb.com/Global/story.asp?S=8275886

[Return to top]

Agriculture and Food Sector

14. *May 7, Lexington Herald-Leader* – (Kentucky) **Worker pleads guilty in food case.** An employee at a Knox County, Kentucky, food-processing plant pleaded guilty Monday to one count of tampering with a consumer product. The woman put a piece of metal in a meatloaf in the hope another employee would be blamed and be fired, according to court documents. The plant managed to recall the meatloaf before it left a distribution center Source: http://www.kentucky.com/779/story/397680.html

15. *May 6, St. Louis Post-Dispatch* – (National) **Problems with imports include tainted seafood, banned drugs.** While China, which has rapidly become the leading exporter of seafood to the U.S., agreed late last year to improve its food export safety, inspectors turned away nearly 400 Chinese shipments of tainted seafood in a year's time, according to Food and Drug Administration records. According to the records, less than one percent of imports are inspected and less than one fifth of that is tested. Seafood is considered one of the riskier imports. When the FDA does turn away shipments, usually it is because they contain veterinary drugs. More than 100 of the shipments were rejected for being filthy, decomposed, or otherwise unfit for consumption. Source: http://www.dallasnews.com/sharedcontent/dws/news/healthscience/stories/DN-foodsafety_05nat.ART.State.Edition1.460b135.html

16. *May 5, Press Democrat* – (California) **Sonoma hit with apple moth quarantine.** After the discovery of a second light brown apple moth in the area last month, a 15-square mile area is under state quarantine in an effort to eradicate the moth from Sonoma County, California. The quarantine means that grape growers, nurseries, and other plant-related businesses in the area are subject to "extensive inspection" and, in some cases, treatment, if their properties are found to be infested. Also, the state forbids residents from taking home-grown fruit, vegetables, plants, and flowers outside of the zone. The state and federal governments have undertaken a $75 million eradication plan that relies largely on aerial spraying of a synthetic pheromone to disrupt the moths mating cycle. Source:http://www1.pressdemocrat.com/article/20080505/NEWS/933937714/1033/NEWS&template=kart

[Return to top]

Water Sector

17. *May 7, Associated Press* – (New Jersey) **DuPont ingredient found in wells near NJ plant.** DuPont says it has found chemical residues from a Teflon ingredient in groundwater near its Chambers Works plant. The traces of the chemical PFOA were found in nine wells around the plant in Deepwater, New Jersey. The concentrations ranged as high as 35 times the alert level established last year by New Jersey regulators. DuPont has stated that there is no evidence of health threats from PFOA, but a federal advisory panel recommended classifying it as a probable carcinogen.
Source:
http://www.philly.com/philly/wires/ap/news/state/new_jersey/20080507_ap_dupontingredientfoundinwellsnearnjplant.html

18. *May 6, Associated Press* – (National) **EPA might not act to limit rocket fuel in drinking water.** An Environmental Protection Agency (EPA) official said Tuesday there is a "distinct possibility" the agency will not take action to rid drinking water of a toxic rocket fuel ingredient that has contaminated public water supplies around the country. Some senators called that unacceptable. They argued that states and local communities should not have to bear the expense of cleansing their drinking water of perchlorate, which has been found in at least 395 sites in 35 states – or the risk of not doing so. The toxin interferes with thyroid function and poses developmental health risks, particularly to fetuses. The assistant administrator for water at the EPA told a Senate hearing that EPA is aware that perchlorate is widespread and poses health risks. But he said that after years of study, the EPA has yet to determine whether regulating perchlorate in drinking water would do much good. He told the chairman of the committee that it was possible that instead of a regulation, the EPA would issue a public health advisory, which would simply provide information. After the hearing, he told reporters that a decision to regulate perchlorate was also still on the table.
Source: http://ap.google.com/article/ALeqM5hkmR-wSU9LKmVT3Iduv0DS9XPTbAD90GAM481

[Return to top]

Public Health and Healthcare Sector

19. *May 7, USA Today*– (National) **Identity thieves prey on patients medical records.** Doctors offices, clinics, and hospitals are a fruitful hunting ground for identity thieves, who are using increasingly sophisticated methods to steal patient information, lawyers and privacy experts say. Legal experts say lawbreakers use medical information to get credit card numbers, drain bank accounts, or falsely bill Medicare and other insurers. The executive director of the advocacy group World Privacy Forum says "sophisticated crime rings" often can make more money by stealing medical identities than by going after individuals' bank accounts or credit cards. In a recent survey of 263 health care providers, 13 percnet said their facility had experienced a data breach. Of those, 56

percent said they notified the patients involved, according to the survey by HIMSS Analytics, a non-profit data analysis firm, and Kroll Fraud Solutions, which offers security-related services. In January, California began requiring that consumers receive notice when their medical information is improperly accessed. Similar legislation is being debated in Congress.
Source: http://www.usatoday.com/news/health/2008-05-06-privacy_N.htm

20. *May 7, Voice of America News* – (International) **WHO to update guidelines for possible flu pandemic.** About 150 experts from governments, the World Health Organization (WHO), and other organizations are meeting to work on new guidelines to help nations confront and combat a potential influenza pandemic. The WHO, which is hosting the week-long meeting, says that it is certain that one day the world will face a human influenza pandemic and that governments must be prepared. But, the coordinator of WHO's Global Influenza Program says the near term risk of an avian influenza pandemic breaking out among humans is anyone's guess. Therefore, he says, it becomes all the more important that governments be prepared to help their people survive a disease that could potentially kill millions. He says advances have been made in the development of an H5N1 vaccine and in anti-viral drugs. He says the World Health Organization has a large stockpile of these drugs and plans are afoot to increase the supply of future vaccines. The meeting this week will focus on areas such as disease control, surveillance, medical interventions, and the role of communications during an influenza pandemic.
Source: http://www.voanews.com/english/2008-05-07-voa9.cfm

21. *May 7, Sun Media* – (International) **Ontario ready for potential SARS-like virus.** Ontario's Health Minister says the province is well prepared to withstand another SARS-like epidemic, following reports that China is dealing with an outbreak of a new virus that has killed at least 26 children. An official with the Ministers office confirmed Canadian Integrated Public Health Surveillance (CIPHS) issued an alert yesterday asking that any unusual clusters or outbreaks of hand, foot, and mouth disease be reported to the agency. Provincial labs are being asked to submit any enterovirus strains that they isolate. Enterovirus 71 (EV-71) is implicated in the more serious cases of hand, foot, and mouth disease that has infected thousands of children in China.
Source: http://lfpress.ca/newsstand/News/National/2008/05/07/5494091-sun.html

22. *May 7, Reuters* – (International) **China child virus cases high but no cause for panic.** China should expect more cases of hand, foot, and mouth disease, but there is no sign it is facing a new or more virulent strain despite an unusually high number of child deaths, officials said on Wednesday. Hand, foot, and mouth is a common childhood illness, but the current outbreak has led to 28 fatalities in China, mostly when linked with enterovirus 71 (EV71), which can cause a severe form of the disease characterized by high fever, paralysis, and meningitis. "There is no indication of a change or a more virulent virus," a World Health Organization China representative told a news conference Wednesday. But he said there were still questions about why there were so many cases in Fuyang, in the eastern province of Anhui, and why they presented unusual symptoms that made it difficult to identify the virus. Chinas official Xinhua

news agency put the number of cases at 15,799, up from about 12,000 cases reported on Tuesday, but the rise was due to more thorough reporting, not the diseases spread, a health official said.
Source: http://ca.reuters.com/article/topNews/idCAPEK14932320080507?sp=true

23. *May 7, Agence France-Presse* – (International) **Vietnam warning on EV71 virus after at least 10 children die.** Vietnams prime minister has urged health authorities to fight a disease outbreak caused by the EV71 virus, which officials Wednesday said had killed at least 10 children this year. "The virus is very contagious," the head of the Health Ministry's Preventive Medicine Department said. "There is a risk of infections from China through infected people moving between China and Vietnam."
Source: http://afp.google.com/article/ALeqM5iliqXKSGq_KkyfRfI3VRhDZq7iTQ

24. *May 6, WFOR 4 Miami* – (Florida) **Feds & lab: No duty to protect public from anthrax.** Lawyers for the federal government and a private laboratory argued Monday before the Florida Supreme Court that they have no duty under Florida law to protect the public from anthrax or other lethal materials. The court will rule on that issue as part of a lawsuit over the death of a man who was exposed to anthrax in 2001 via an envelope sent through the mail.
Source: http://cbs4.com/local/national.enquirer.star.2.716948.html

Government Facilities Sector

25. *May 7, Washington Post* – (National) **U.S. tests response to set of calamities.** Thousands of key federal employees are being whisked from the Washington area by helicopter and car for a three-day test of their ability to run the government from remote locations during a disaster. The exodus, which began yesterday and will continue today, involves the White House and other parts of the executive branch. Congress and the judiciary are not part of the exercise, which is being overseen by the Department of Homeland Security. This weeks "continuity of government" drill is one of the largest by the federal government since 9/11, officials said. It is part of a national eight-day exercise in which officials are responding to a cascade of nightmarish events. The drill started Thursday, with terrorists sabotaging a tanker carrying poisonous gas in Washington state. Next, suspected nerve gas was accidentally released from a government stockpile in Oregon. The disaster script also calls for a devastating Category 4 hurricane to roar up the East Coast toward the District, where officials will be getting word of a terrorist threat to the capital. Officials leaving the Washington area will work from temporary offices in Virginia, West Virginia, and Maryland for periods ranging from a few hours to two days. Others will work from home.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/05/06/AR2008050602687.html

26. *May 6, KOAT 7 Albuquerque* – (New Mexico) **Santa Fe building evacuated due to bomb threat.** State and Santa Fe police have evacuated the Joseph Montoya Building because of a bomb threat. The threat was received around 4 p.m. Tuesday, and the

building was immediately evacuated. State police bomb-sniffing dogs are being used inside and outside the building. The building houses offices for the General Services Departments Building Services, Property Control, and Risk Management Divisions, as well as some offices of the Economic Development Department.
Source: http://www.koat.com/news/16180723/detail.html

27. *May 6, Hutchinson Leader and Litchfield Independent Review* – (Minnesota) **Bomb squad detonates explosive device in Eden Valley.** The Meeker County, Minnesota, Sheriffs Office called the Minneapolis Bomb Squad to the Eden Valley City Hall Tuesday morning after a man brought an explosive device into the building. At 9:34 a.m., the sheriff's office received a report from Eden Valley Police that a man found an explosive device while cleaning out a storage shed. He brought it to the City Hall-Police Department building, which was then evacuated. The Minneapolis Bomb Squad arrived on the scene two hours later to remove, secure, and disable the bomb at a remote location. A landlord had found the device, which resembled a pipe bomb, while cleaning out a storage area of a rental property. The sheriff's office will submit materials collected from the device to the U.S. Bureau of Alcohol, Tobacco and Firearms for testing. An investigation is ongoing.
Source: http://www.hutchinsonleader.com/news/police/bomb-squad-detonates-explosive-device-eden-valley-7911

28. *May 6, New York Times* – (New York) **Report faults city on potentially toxic school sites.** In a 17-page report released Tuesday, a New York City public advocate contended that a loophole in state law had permitted the city's School Construction Authority "to open schools on potentially toxic sites that could pose a health threat for New York City schoolchildren." But the city's Education Department immediately disputed the reports findings, insisting that it had not placed any students at risk from environmental pollutants. The report focuses on schools housed in buildings leased by the authority. Some of the buildings have been found to be contaminated with toxins like perchloroethylene, trichloroethylene, and lead, but the State Department of Environmental Conservation determined that the levels were not high enough to make the buildings unsafe for use as schools. The report does not assert that children are actively at risk, but contends that the authority was able to lease the sites "without community notification, environmental review, or City Council oversight."
Source: http://cityroom.blogs.nytimes.com/2008/05/06/report-faults-city-on-potentially-toxic-school-sites/

29. *May 6, TG Daily* – (District of Columbia) **As many as 1000 laptops missing from State Department.** Several hundred to possibly a thousand laptops are missing from the U.S. State Department, according to an internal audit. Many of the laptops likely contain classified information, and as many as 400 computers belonged to the Anti-Terrorism Assistance Program which provides counterterrorism training to other nations. According to CQ Politics, the department has dispatched vans to locations throughout the Washington D.C. area in an attempt to locate and recover the missing computers. According to one source, up to $30 million in equipment is missing, and laptops comprise 99 percent of that total. The audit is still in its early stages, and it is

likely that the missing laptop count will rise.
Source: http://www.tgdaily.com/content/view/37292/108/

30. *May 6, Associated Press* – (Indiana) **3 Obama campaign offices searched after bomb threat.** Authorities have evacuated and searched three Barack Obama campaign offices in Indiana in response to a bomb threat that was made while people voted in the states primary. The bomb threats made against offices in Terre Haute, Vincennes, and Evansville were reported Tuesday in a call to a Terre Haute television station. The reports mirror the circumstances of Obama's office in Vincennes being vandalized early Monday morning. In that incident, a male caller also reported the vandalism to a station in Terre Haute.
Source:
http://ap.google.com/article/ALeqM5i44gg2bbRqtgiMH1V0tsickBx3TwD90GDDP00

31. *May 6, Information Week* – (National) **Manhole covers: Gateways to terrorism.** Manhole Barrier Security Systems warned on Monday that cities need to do more to protect against assaults on infrastructure launched by underground attackers. The company's chairman and chief executive officer argues that it is too easy for terrorists and vandals to enter the subterranean world, where telecommunications and utility lines are buried. This view was also confirmed by a former commissioner of the U.S. Presidents Commission on Critical Infrastructure Protection, who wrote a report titled "Manhole Security: Protecting Americas Critical Underground Infrastructure." In it, he warns, "Without manhole security, the United States risks suffering significant consequences resulting from an attack on underground infrastructure, including incalculable economic damages, large numbers of civilian casualties, and considerable disruptions to our urban way of life."
Source:
http://www.informationweek.com/blog/main/archives/2008/05/manhole_covers.html

[Return to top]

Emergency Services Sector

32. *May 6, Reno Gazette-Journal* – (Nevada) **Response teams train for disaster.** The 95th Weapons of Mass Destruction Civil Support Team from Hayward, California, and the 92nd Weapons of Mass Destruction Civil Support Team from Las Vegas (both National Guard Civil Support Teams) took part in a drill Monday along with the Reno Fire Department, responding to a report of a suspicious odor near Reno-Tahoe International Airport. The National Guard teams are in Reno this week training with Reno's Hazardous Materials Response Team for chemical, biological, radiological, explosive, and nuclear events. Operation Joint Support was staged Monday at the Nevada Air National Guard base near the airport. Similar training will occur Wednesday near the Stead Airport in north Reno. A Reno Fire Department spokesman said the training exercises allow the hazardous material teams and the National Guard teams to learn about each others abilities and how to improve their interaction.
Source:
http://www.rgj.com/apps/pbcs.dll/article?AID=/20080506/NEWS04/805060350/1321/N

EWS

[Return to top]

Information Technology

33. *May 7, ComputerWeekly.com* – (International) **Major media malware attack breaks out on file-sharing networks.** McAfee has reported "the most significant malware outbreak in three years," with more than 500,000 detections of a Trojan horse masquerading as a media file. Since Friday 2 May, more than 500,000 instances of the Trojan have been detected on PCs. The malicious MP3 music or Mpeg video files have appeared on popular file-sharing services such as Limewire and eDonkey. Firms should be concerned as employees often access such file-sharing networks on corporate machines. Security software firm McAfee rates the threat as a "medium" risk. No other malware has received that risk rating since 2005. All other threats since then have been rated lower on the severity scale. "This is one of the most prevalent pieces of malware in the past three years," said a threat researcher at McAfee Avert Labs. "We have never before had a threat this significant that arrives as a media file." Cybercrooks have loaded hundreds of rigged MP3 and Mpeg files on to file-swapping services. The files are all named differently in multiple languages, and vary in size to make them appear like legitimate music or video files. Attempting to play one of the malicious files will trigger the download of an application named "PLAY_MP3.exe", which will serve ads to the infected computer. McAfee identifies the Trojan horse as "Downloader-UA.h." Some of the sample names used by the malicious media files include "preview-t-3545425-adult.mpg", "preview-t-3545425-changing times earth wind.mp3", "preview-t-3545425-girls aloud st trinnians.mp3", "preview-t-3545425-jij bent zo jeroen van den.mp3", "t-3545425-lion king portugues.mpg" and "t-3545425-los padres de ella.mpg".
Source: http://www.computerweekly.com/Articles/2008/05/07/230582/major-media-malware-attack-breaks-out-on-file-sharing.htm

34. *May 6, Dark Reading* – (National) **University study examines the causes and costs of hard drive failure.** Viruses or Trojans can infect PCs and wreck their hard drives. But how often does it really happen – and how bad is the damage? A new university study suggests that hard-drive-killing attacks launched by hackers are rare – but when they do occur, they can be more costly than most companies think. The study, published last quarter by professors at the University of Pepperdine and commissioned by data recovery vendor Deepspar Technologies, looks at the causes of hard drive failure and offers insights on just how "fatal" a fatal drive error can be. Aside from physical theft, hard drive failure is the most common cause of data loss on PCs, the study says, accounting for 38 percent of data loss incidents. In about 30 percent of these cases, the loss of access is the result of drive problems, where corruption of the media makes the data unreadable. Software corruption, which is the usual path used by hackers and viruses to "crash" a hard drive, only causes data loss in about 13 percent of cases. Such incidents are only slightly more frequent than drive losses caused by human error (12 percent). But while remote attacks may cause fewer crashes than many users believe, the cost of the crashes may be higher than many executives expect, the study states.
Source: http://www.darkreading.com/document.asp?doc_id=153090

35. *May 6, Medical News Today* – (International) **A digital haven for terrorists on our own shores?** If you use one of Americas top Internet service providers, you may share server space with an organization that enables worldwide terrorism, says a new study by Tel Aviv University. A workshop on terrorist organizations and the Internet was organized for the North American Treaty Organization (NATO) by the Netvision Institute for Internet Studies (NIIS) and the Interdisciplinary Center for Technology Analysis & Forecasting, both of Tel Aviv University. Berlins Institute for Cooperation Management and Interdisciplinary Research (NEXUS), affiliated with the Technical University of Berlin, also participated. The findings were presented in Berlin to a closed audience of high-ranking representatives from NATO in February 2008. Enlisted by NATO officials to study the web activity of terrorist organizations, researchers found that some of the worlds most dangerous organizations are operating on American turf. Hezbollah, the Islamic Jihad, and al-Qaeda all have websites hosted by popular American Internet service providers - the same companies that most of us use every day. Source: http://www.medicalnewstoday.com/articles/106423.php

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

36. *May 6, Reuters* – (International) **Verizon joins another undersea cable network.** Verizon Communications Inc's business unit said on Tuesday it would help build an undersea cable connecting Europe, the Middle East and India to expand its global network to support Internet traffic. Verizon Business, the company's unit in charge of corporate clients, said it joined a consortium of 16 companies to build a 9,000 mile optical cable system linking the three continents. The network, named the Europe India Gateway, is due to be completed in 2010 and cost more than $700 million. The unit did not disclose how much it would pay. Verizon Business is involved in more than 67 submarine cables worldwide, and the Europe India Gateway is its third major project in the last four years. It has been boosting advanced cable network investment to provide more stable voice connections and faster Internet services for global corporate clients. Source: http://www.reuters.com/article/technologyNews/idUSN0650770720080506

[Return to top]

Commercial Facilities Sector

Nothing to Report

[Return to top]

National Monuments & Icons Sector

Nothing to Report

[Return to top]

Dams Sector

37. *May 7, Sierra Sun* – (California) **Recent quakes havent shaken at-risk dam near Truckee.** Seismic study is high priority at the Martis Creek Dam in California, but recent earthquakes in the area have not affected the safety of structure. Located three miles east of Truckee in the Martis Valley, the earthen-fill dam has been categorized as an "extremely high risk" by the U.S. Army Corps of Engineers for seepage issues. Geologists blame the coarse glacial soil for the seepage that could destabilize the dam, making it one of the six riskiest dams in the nation. Because of that risk, officials are keeping water levels low. Meanwhile, the potential of nearby active faults also compound the risk the dam poses to downstream residents through the Truckee River Canyon, in Reno and Sparks, Nevada. An initial study released in March indicated a recently-active fault may lie underneath the dam itself. According to a May 2 situation report from the Corps, investigation of that fault will occur this summer.
Source: http://www.sierrasun.com/article/20080507/NEWS/637325575

38. *May 7, Edmonton Sun* – (International) **Oilsands ponds concern security expert.** The oilsands tailings ponds in Alberta, Canada, are a magnet for a massive terrorist attack, a Toronto-based security consultant is warning. "Were basically a target for international terrorist groups. But because we provide most of the (United States) fuel, that makes us an even bigger concern," said a consultant from Globe Risk Holdings. The security consultant, who was part of a group of consultants that prepared a report for the Alberta government on the terrorist threat, said a big worry is that attackers could try to breach the dams that hold the toxic tailings, thus sending them into the nearby Athabasca River north of Fort McMurray. His other concern is that in his view, companies have not done enough to prepare for an attack. Provincial officials, however, disagree. Alberta's chief sheriff said the government rejected the consultants report because many of its conclusions were based on speculation and not on facts. But while he admits tailings ponds could attract terrorists interest, the sheriff is confident the oilsands companies are taking steps to protect their facilities. "The government of Alberta believes that there are significant mitigating strategies in place to prevent that from happening," he said.
Source: http://www.edmontonsun.com/News/Alberta/2008/05/07/5493031-sun.html

39. *May 6, Alton Telegraph* – (Illinois) **Corps closes auxiliary chamber at Mel Price Locks and Dam.** In Illinois, the 600-foot-long auxiliary chamber at the Melvin Price Locks and Dam 26 remained closed Tuesday, awaiting an inspection of a malfunction with the upstream miter gates. The U.S. Army Corps of Engineers St. Louis District announced the closure to the river navigation industry Monday. As a result, all river traffic will be routed through the 1,200-foot-long main chamber, which will remain open throughout the closure of the auxiliary chamber. The reason for the closure is an

inability to fully recess the upstream miter gates into the lock walls of the auxiliary chamber. This makes it impossible for barge tows to enter and exit the chamber safely. When opened all the way, the miter gate leafs are supposed to be flush with the lock walls. Debris from high water levels on the Mississippi River may be preventing the upstream miter gates from opening fully, Corps officials said. Efforts were made to clear debris or silt over the weekend, using both pneumatic and mechanical means, but they were unsuccessful.
Source:
http://www.thetelegraph.com/news/chamber_13793___article.html/miter_gates.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer